

Чек-лист выбора подрядчика по ИИ: 10 вопросов до подписания договора

Зачем этот лист. Оператор персональных данных - вы, а не подрядчик и не поставщик модели: перед вашим работником отвечаете вы (ч. 5 ст. 6 152-ФЗ). Договор эту ответственность не перекладывает - он определяет лишь, что вы сможете потребовать с подрядчика потом. Поэтому вопросы задаются **до** подписания, а ответы фиксируются в договоре, а не в переписке. **Три и больше «красных флагов» - ищите другого подрядчика.**

Три уровня защиты

1 · Обезличивание

Роли вместо фамилий, фрагмент вместо файла. Вручную - ноль рублей, автоматически - ИИ-шлюз с маскированием

2 · Российский хостинг

Отвечает на вопрос «где лежат данные», но не на «на каком основании» и «в каком составе»

3 · Контур компании

Модель внутри вашей сети; сервер можно купить или взять по подписке. Для спецкатегорий, биометрии, всей кадровой базы

Вопросы 1-5

1 Где физически хранятся и обрабатываются данные - и кто ещё в цепочке?

За подрядчиком стоят поставщик модели, облако, сервис расшифровки. Каждый - отдельное лицо, получающее данные ваших людей.

ХОРОШИЙ ОТВЕТ

Называет страну и площадку, даёт письменный перечень всех, кто получает данные, и сообщает об изменениях

ч. 5 ст. 18 · ст. 12 152-ФЗ - локализация и трансграничная передача

КРАСНЫЙ ФЛАГ

«Данные в облаке», «это наш внутренний вопрос», отказ назвать поставщика модели

2 Кто из нас оператор, кто обработчик - и есть ли поручение на обработку?

Отдать данные подрядчику на обработку можно только по поручению с обязательным набором условий. Пользовательское соглашение сервиса поручением не является.

ХОРОШИЙ ОТВЕТ

Поручение со всеми обязательными условиями плюс согласие работников, где этот обработчик назван

ч. 3 ст. 6 · п. 6 ч. 4 ст. 9 152-ФЗ - поручение и согласие

КРАСНЫЙ ФЛАГ

«В договоре всё есть» без отдельного поручения; «мы не обрабатываем ПДн» - при том что в систему грузят файлы с фамилиями

3 Обучается ли модель на наших данных? Что с журналами запросов?

Отозвать данные, попавшие в чужую модель, нельзя - в отличие от партии деталей.

ХОРОШИЙ ОТВЕТ

Запрет обучения на ваших данных прямо в договоре; назван срок хранения журналов запросов

КРАСНЫЙ ФЛАГ

«Модель ничего не запоминает» без пункта договора; срок хранения журналов не определён

4 Кто отвечает, если утечёт у подрядчика?

Перед работником и регулятором отвечаете вы. Взыскать с подрядчика убытки реально, если его обязанности по защите прописаны в договоре.

ХОРОШИЙ ОТВЕТ

Подрядчик возмещает штрафы и претензии работников при инциденте у себя; уведомление об инциденте - немедленно, счёт идёт на часы

ч. 5 ст. 6 152-ФЗ · ч. 3.1 ст. 21 - 24 и 72 часа на уведомление · ст. 406.1 ГК РФ - возмещение потерь

КРАСНЫЙ ФЛАГ

Лимит ответственности - месячная стоимость услуг; «уведомим в разумный срок»

5 Чем подтверждается защита: лицензии, модель угроз, уровень защищённости?

Аттестация системы коммерческой компании не обязательна, а оценка эффективности мер - обязательна. Расходы на защиту силами лицензиатов - единственный в законе способ снизить оборотный штраф.

ХОРОШИЙ ОТВЕТ

Показывает модель угроз, уровень защищённости и - если работает с защитой информации - лицензию ФСТЭК

ст. 19 152-ФЗ · ПП РФ № 1119 · приказ ФСТЭК № 21 · ч. 3.4-2 ст. 4.1 КоАП

КРАСНЫЙ ФЛАГ

«Мы соответствуем 152-ФЗ» без единого документа; сертификат, выданный самому себе

Вопросы 6-10

6 Что происходит с данными, когда мы расстаёмся?

Правильный ответ - не «мы всё удалим», а два документа, которые вы получите на руки.

ХОРОШИЙ ОТВЕТ

Акт об уничтожении и выгрузка из журнала регистрации событий; назван срок и формат возврата данных, а у сервера по подписке - что будет с дисками

ч. 4 ст. 21 152-ФЗ - 30 дней • приказ РКН № 179 - состав подтверждающих документов, хранить 3 года

КРАСНЫЙ ФЛАГ

«Конечно, удалим» без документов; молчание про журнал регистрации событий

7 Кто принимает кадровое решение - человек или модель?

Ограничение Трудового кодекса жёстче: в 152-ФЗ запрет снимается письменным согласием, в ТК для работников - ничем.

ХОРОШИЙ ОТВЕТ

Система даёт рекомендацию с объяснением, решение фиксирует человек, основание отказа можно изложить письменно

п. 6 ст. 86 ТК РФ • ст. 16 152-ФЗ • ст. 64 ТК РФ - 7 рабочих дней на обоснование отказа

КРАСНЫЙ ФЛАГ

«Система сама отсеет неподходящих»; нельзя объяснить, почему у кандидата низкий балл

8 Чьё останется то, что сделано: промпты, настройки, интеграции?

Одно предложение в предмете договора решает, сможете ли вы сменить подрядчика, не начиная заново.

ХОРОШИЙ ОТВЕТ

Права на созданное по заказу - ваши; сопровождение можно передать другому; всё выгружается в открытом формате

ст. 1296 ГК РФ - права заказчику • ст. 1297 ГК РФ - права подрядчику

КРАСНЫЙ ФЛАГ

«Это наша методология»; настройки живут только у подрядчика; выгрузка «невозможна»

9 Кто конкретно будет работать и какие доступы получит?

Данные утекают не через архитектуру, а через людей и забытые учётные записи.

ХОРОШИЙ ОТВЕТ

Поимённый список и именные учётки, NDA с сотрудниками, порядок выдачи и отзыва доступов, включая удалённый, согласование субподряда

КРАСНЫЙ ФЛАГ

Общая учётка на команду; «часть работ на аутсорсе» без имён; бессрочный или постоянный удалённый доступ

10 Какой уровень нужен именно нам - и почему?

Единственный вопрос, на который здесь нет готового ответа: он зависит от того, что лежит в вашем кадровом контуре. Медосмотры - специальная категория данных, проходная с распознаванием лица - биометрия. Порога «от тысячи человек» для них нет: утечка значима, даже если пострадал один человек.

КАК ОТВЕТИТЬ САМИМ

Выпишите процессы, где нужен ИИ, и против каждого - что попадёт в текст: фамилии, здоровье, биометрия, зарплаты. Уровень задаёт самая чувствительная строка

ст. 10 и ст. 11 152-ФЗ • ч. 16 и ч. 17 ст. 13.11 КоАП - порога по числу людей нет

КРАСНЫЙ ФЛАГ

Подрядчик предлагает уровень, не спросив, какие категории данных вы обрабатываете

Что можно сделать в понедельник, бесплатно

1. Откройте последний файл, который отправляли в нейросеть, и посмотрите, сколько там фамилий.
2. Договоритесь в команде о простом правиле: в чат уходят роли и цифры, а не фамилии, телефоны и оклады. Не файл целиком, а нужный фрагмент.
3. Проверьте, на какой приказ ссылается ваша политика обезличивания: приказ Роскомнадзора № 996 от 05.09.2013 отменён, с 01.09.2025 действует приказ № 140 от 19.06.2025.
4. Выясните, кто у вас отвечает за организацию обработки персональных данных, и убедитесь, что он знает про ИИ-сервисы.

ДЕСЯТЫЙ ВОПРОС

На девять вопросов ответы здесь. Десятый зависит от того, что именно лежит у вас в кадрах. Хотите разобрать его на своём случае или научить команду работать с ИИ безопасно - напишите.

